GUÍA DEFINITIVA PARA ADAPTARSE AL NUEVO REGALMENTO EUROPEO DE PROTECCIÓN DE DATOS (GDPR)

MAYO 2018

vanadis©

GDPR (General Data Protection Regulation)

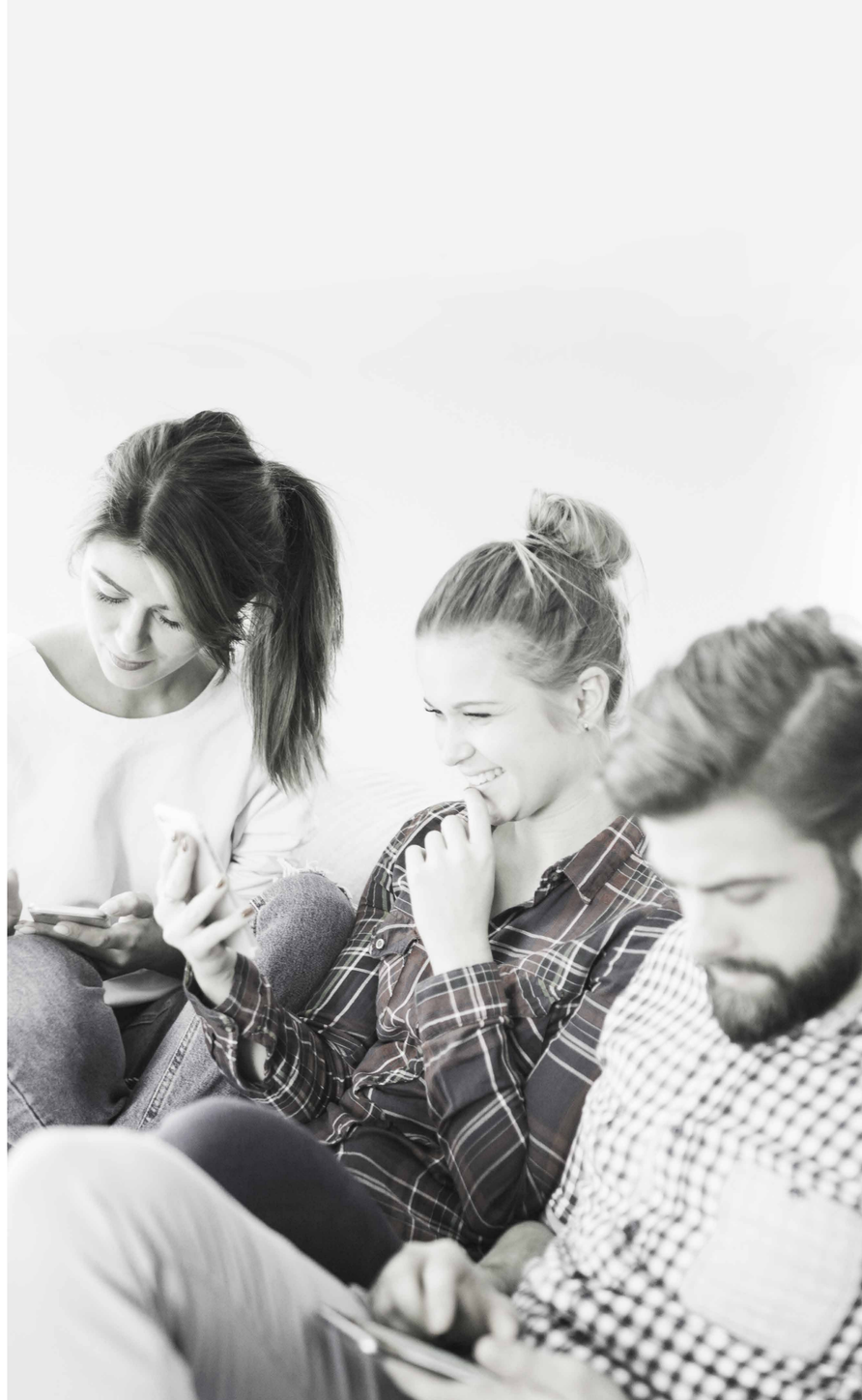
Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación
de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Esta normativa regulará la protección de datos de los europeos a partir del 25 de mayo de 2018. Este reglamento pretende fortalecer los derechos de privacidad de las personas y busca mejorar la seguridad y protección de los datos de los

¿Por qué nace esta iniciativa?

*Al **70%** de los europeos les preocupa que las empresas puedan utilizar la información para fines diferentes de aquellos para los que se ha protegido.*

*El **90%** de los europeos cree que es importante que en todos los países de la UE se tengan los mismos derechos y la misma protección.*



7 Princios que las empresas deberán conocer para adaptarse a la GDPR?

7 principios de obligado cumplimiento para todas aquellas empresas que manejan datos de caracter personal de ciudadanos de la Unión Europea.

1. Todas las empresas deberán redactar **nuevas cláusulas de protección de datos**. Aparecen nuevos derechos: derecho a la portabilidad o derecho al olvido.

2. Será necesario **redactar nuevos contratos** con los encargados del tratamiento de datos, debido a que con el nuevo reglamento aparecen nuevas obligaciones para ellos.

3. Todas las empresas deberán realizar un **análisis de riesgos** desde el punto de vista de la protección de datos.

4. Es obligatorio **comunicar** a la **Agencia Española, Catalana o Vasca de Protección de Datos** cualquier **brecha de seguridad** en un plazo de **72 horas.**

5. Aparece en las empresas la nueva figura del **Delegado de Protección de Datos**, que estará certificada en un futuro.

5. Se **unificarán** todas las **normativas europeas** de protección de datos.

6. Aumento de las sanciones desde el 4% de la facturación de la empresa en el ejercicio anterior hasta los **20.000 millones de euros**.

¿A qué datos afecta la ley GDPR?

La GDPR afecta a la recogida, tratamiento, gestión yretención de todos los datos de caracter personal de individuos de la unión Europea.

¿Qué se consideran datos personales?

Los datos personales que contempla la GDPR se definen como "... Cualquier información relativa al individuo, tanto de su vida privada, pública o profesional, que puede ayudar a identificar a una persona tanto directa como indirectamente"... Entendemos como datos personales el **nombre**, una **foto**, una **dirección de correo electrónica**, **datos bancarios**, **publicaciones en redes sociales**, **información médica** o la propia **dirección IP** de los dispositivos desde los que se conecta a internet.

Tratamiento de datos sensibles:

Aquellos que representan un **alto riesgo a los derechos y libertados de la persona** y que puedan ayudar a identificar a una persona tanto directa como indirectamente: que puedan llevar a la discriminación de una persona, relativos a su situación financiera, credenciales de acceso como contraseñas o usuarios, datos de secreto profesional o protegidos legalmente y datos que puedan ocasionar un fraude de identidad.

Tratamiento de datos especiales:

La GDPR **prohibe estrictamente el tratamiento de datos especiales** salvo en ciertas excepciones acordadas con el usuario (Sanidad, instituto de empleo, etc). Se consideran datos especiales los que revelan el origen racial o étnico, opiniones políticas o religiosas, datos genéticos, relativos a la salud, de la orientación sexual o acerca de delitos y condenas.

Fases de aplicación de la GDPR

La empresa deberá atender regularmente la protección de los datos **en todas las fases de su ciclo de vida**, desde la obtención hasta el tratamiento, gestón y la conservación de los mismos.

¿A qué datos afecta la ley GDPR?

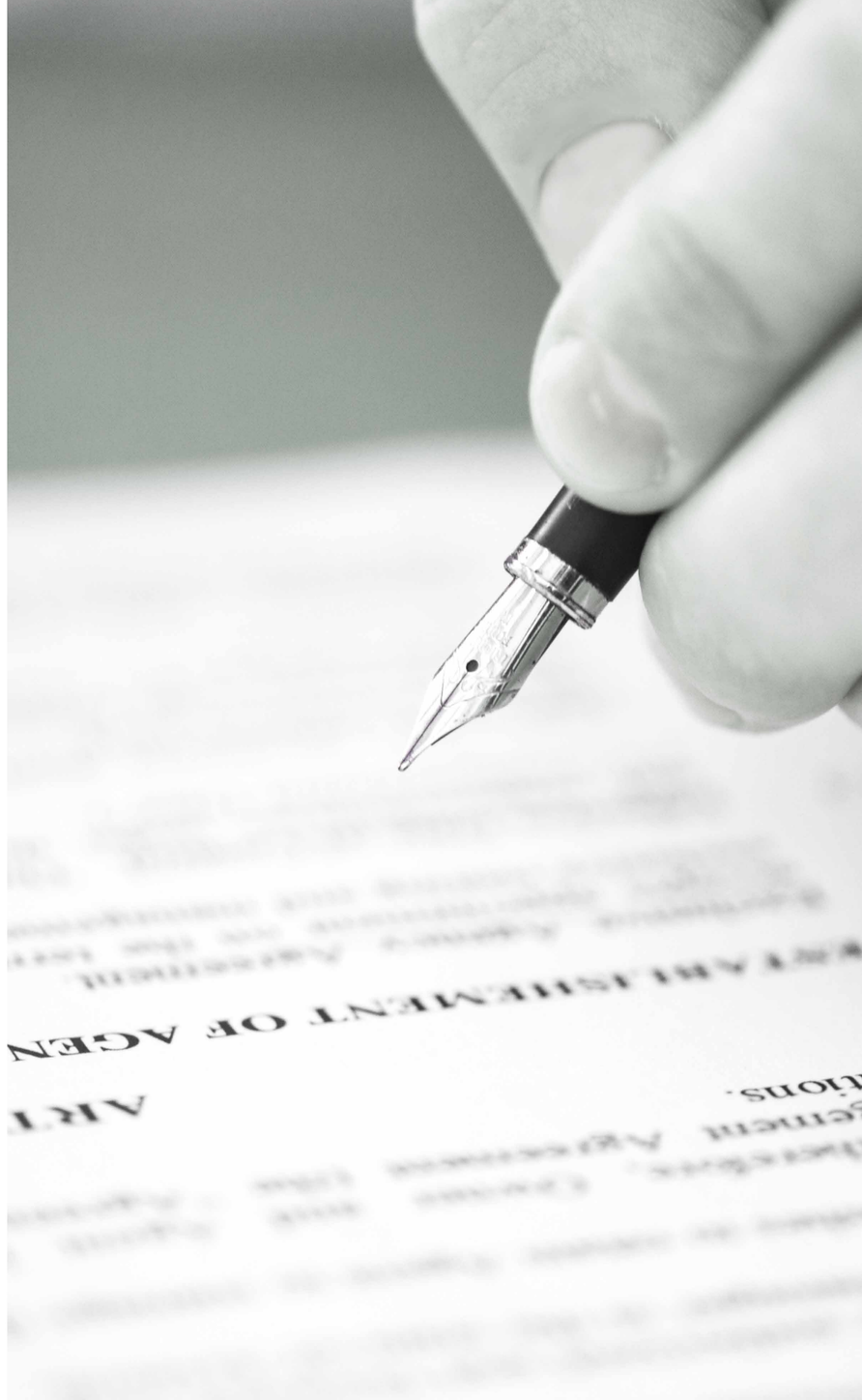
LA OBTENCIÓN DE DATOS PERSONALES

La obtención de los datos personales deberá de obedecer a tres criterios de protección:

Justa: los datos deberán de ser pertinentes para con la actividad de la empresa.

Legítima: se solicitará el consentimiento a los interesados y estos deberán aceptar las condiciones.

Explícita: se informará en todo momento del uso y finalidad de los datos que se soliciten.



¿A qué datos afecta la ley GDPR?

TRATAMIENTO DE LOS DATOS

Para el tratamiento de los datos personales se deberán tener en cuenta los siguientes aspectos:

El dato tiene que ser **objetivo de la actividad económica** para la que se ha solicitado.

Si la **finalidad del uso** de los datos **cambia** la empresa deberá informar al usuario y este deberá aceptar de nuevo tales cambios.

¿A qué datos afecta la ley GDPR?

GESTIÓN DE LOS DATOS

Para la correcta gestión de los datos personales se deberña cumplir con los siguientes requisitos:

El ciudadano tendrá **acceso en todo momento** a sus datos personales.

Se le concederá el derecho a **rectificarlos** siempre que lo considere.

Se le dará **derecho al olvido**. El usuario puede exigir que sus datos no aparezcan en la bases de datos y la empresa deberá ofuscarlos.

La **transferencia de datos fuera de la UE** es **libre y legal** salvo excepciones reguladas mientras que el proveedor haya firmado un acuerdo con la UE.

¿A qué datos afecta la ley GDPR?

CONSERVACIÓN Y SEGURIDAD DE LOS DATOS

Criterios de conservación de los datos:

El tiempo de tratamiento de los datos no será indefinido.

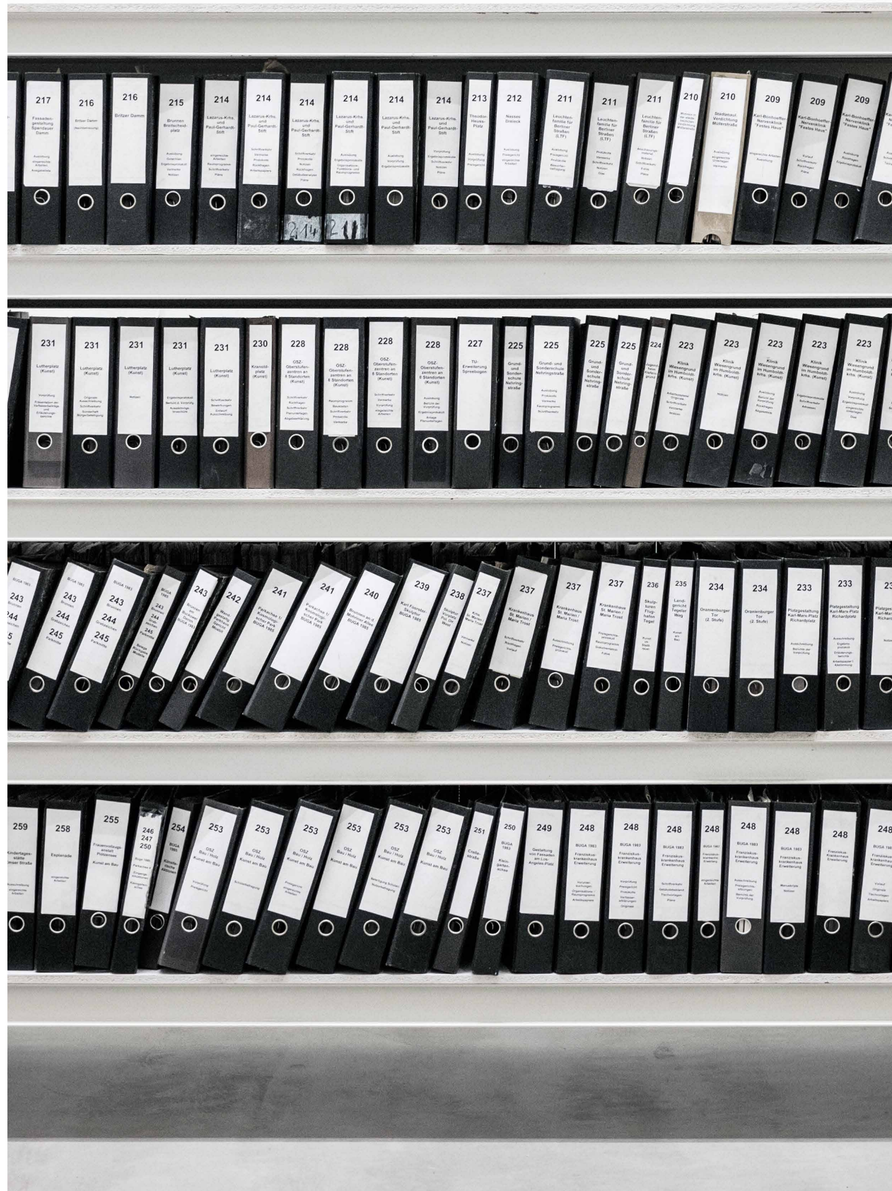
Los datos podrán ser almacenados siempre que tengan un **objetivo relacionado con la actividad económica** para la que fueron obtenidos.

En caso contrario, no es obligatorio borrar los datos porque estos puedan ser requeridos a la empresa en un futuro. La normativa no obliga a borrar, sino a **ofuscar los datos**. Esto quiere decir que los datos no deberán estar almacenados en la base de datos ni tampoco se podrá hacer uso de ellos.

Criterios de seguridad:

La empresa deberá **velar por la seguridad durante todo el ciclo de vida de los datos**: se utilizarán login seguros, aplicaciones seguras, una base de datos protegida, entornos web seguros, etc.

Será recomendable la combinación de **varias tecnologías** para lograr adaptar todos los procesos que realicemos al nivel de seguridad que exige la normativa.



¿Con qué perfiles debo contar en mi empresa?

DATA PROTECTION OFFICER

DPO, es el responsable de la implantación y ejecución de la ley en la emrpesa.

Perfil de caracter legal como un **abogado** o **gestor**.

DATA PROCESSOR

Encargado del tratamiento de la información en el día a día de la epresa.

DATA CONTROLLER

Responsable del tratamiento de la información.

La violación de seguridad de los datos personales

¿QUÉ OCURRE CUANDO HAY UN FALLO?

¿A quién debo notificarlo?

En el caso de que se produzca un fallo de seguridad, los responsables deberán comunicarlo a la **Agenica Española, Catalana o Vasca de Protección de Datos (AGPD)** en un plazo de **72 horas**; además, deberá informar a los afectados en caso de que exista algún riesgo para sus derechos.

¿Qué considera la GDPR como violación de datos personales?

La violación de seguridad de datos personales incluye la **pérdida**, **destrucción** o **alteracción** de estos, el **tratamiento de otra forma** no aceptado por el usuario o el **acceso no autorizado** a los mismos.

¿Cuáles son las sanciones por incumplimiento de la GDPR?

Las multas ascienden desde el **4% del volumen de facturación anual** hasta un **máximo de 20 millones de euros**.

¿En qué punto de adaptación a la GDPR se encuentra mi empresa?

LAS PREGUNTAS QUE MI EMPRESA DEBERÍA HACERSE

- Estamos recogiendo los datos que marca la ley?
- Estamos recogiendo datos que no persiguen un objetivo para la empresa?
- Tenemos el conocimiento de dónde están almacenados los datos?
- Qué copias existen de los datos?
- Quién los está tratando y quién tiene acceso a ellos?
- Tenemos aplicaciones seguras y preparadas para Privacy Design?
- Tenemos normativas internas para gestionar los nuevos cambios de la GDPR?
- Tenemos procedimientos de detección y respuesta para mitigar los riesgos?

Servicio de Asesoría Legal

En **Vanadis** somos experos en Consultoría Tecnológica y Desarrollo de Software a Medida. Desde hace más de 10 años trabajamos con las tecnologías más seguras del mercado.

Para garantizar la seguridad y tranquilidad de nuestros clientes ofrecemos el **Servicio de Asesoría Legal para el Cumplimiento de la GDPR**.

¡Llámanos y te informaremos!
911 163 882

O escríbenos a **info@vanadis.es**

vanadis©

www.vanadis.es
info@vanadis.es
@VanadisApps

VANADIS CENTRAL
C/ Gaztambide 65 B
28015 - Madrid
911 163 882

VANADIS SUR
Campus Científico Tecnológico
Ed. Incubadora Empresas.
Despacho 11
23700 - Linares (Jaén)
953 820 980